

A Construction for Perfect Periodic Autocorrelation Sequences

Samuel T. Blake, Andrew Z. Tirkel

School of Mathematical Sciences, Monash University, Australia

ABSTRACT. We introduce a construction for perfect periodic autocorrelation sequences over roots of unity. The sequences share similarities to the perfect periodic sequence constructions of Liu, Frank, and Milewski.

Perfect periodic autocorrelation sequences see applications in many areas, including spread spectrum communications [Simon, 1985], channel estimation and fast start-up equalization [Milewski, 1983], pulse compression radars [Farnett, 1990], sonar systems [Xu, 2011], CDMA systems [Ipatov, 2005], system identification [Van Schyndel, 2001], and watermarking [Tirkel, 1993].

There exists a number of known constructions for perfect sequences over roots of unity. These include Frank sequences of length n^2 over n roots of unity [Heimiller, 1961][Frank, 1962], Chu sequences of length n over n roots of unity for n odd and length n over $2n$ roots of unity for n even [Chu, 1972], Milewski sequences of length m^{2k+1} over m^{k+1} roots of unity [Milewski, 1983], Liu-Fan sequences of length n over n roots of unity for n even [Liu, 2004]. Other sequence constructions exist [Ipatov, 1979][Alltop, 1980][Lewis, 1982][Kumar, 1985][Gabidulin, 1993][Mow, 1993]. This construction presented in this paper is similar to the ZCZ sequence construction by the authors [Blake, 2012].

The periodic cross-correlation of the sequences, $\mathbf{a} = [a_0, a_1, \dots, a_{n-1}]$ and $\mathbf{b} = [b_0, b_1, \dots, b_{n-1}]$, for shift τ is given by

$$\theta_{\mathbf{a}, \mathbf{b}}(\tau) = \sum_{i=0}^{n-1} a_i b_{i+\tau}^*,$$

where $i + \tau$ is computed modulo n . The periodic autocorrelation of a sequence, \mathbf{s} for shift τ is given by $\theta_{\mathbf{s}}(\tau) = \theta_{\mathbf{s}, \mathbf{s}}(\tau)$. For $\tau \neq 0 \bmod n$, $\theta_{\mathbf{s}}(\tau)$ is called an *off-peak* autocorrelation. A sequence is *perfect* if all off-peak autocorrelation values are zero.

The periodic autocorrelation of a sequence, $\mathbf{s} = [s_0, s_1, \dots, s_{ld^2-1}]$, can be expressed in terms of the autocorrelation and cross-correlation of an array *associated* with \mathbf{s} [Heimiller, 1961][Frank, 1962][Mow, 1993]. The sequence \mathbf{s} has the *array orthogonality property* (AOP) for the *divisor* d , if the array \mathbf{S} associated with \mathbf{s} has the following two properties:

1. For all τ , the periodic cross-correlation of any two distinct columns of \mathbf{S} is zero.
2. For $\tau \neq 0$, the sum of the periodic autocorrelation of all columns of \mathbf{S} is zero.

Any sequence with the AOP is perfect [Mow, 1993].

In most perfect sequence constructions, one proves the sequence has perfect autocorrelation by reducing the autocorrelation to a Gaussian sum. A Gaussian sum is given by $\sum_{k=0}^{n-1} \omega^{qk}$, where $\omega = e^{2\pi\sqrt{-1}/n}$ and $q \in \mathbb{Z}$. If $q \neq 0 \bmod n$, then the sum is zero.

We present a construction for perfect sequences over roots of unity. Let \mathbf{s} be a sequence of length $4mn^{k+1}$ over $2mn^k$ roots of unity, where $n, m, k \in \mathbb{N}$. Construct a $2mn^{k+1} \times 2$ array, \mathbf{S} , over $2mn^k$ roots of unity, where $\mathbf{S} = [S_{i,j}] = \omega^{\lfloor i(i+j)/n \rfloor}$ and $\omega = e^{2\pi\sqrt{-1}/(2mn^k)}$. The sequence \mathbf{s} is constructed by enumerating, row-by-row, the array \mathbf{S} .

We now show that \mathbf{s} has perfect periodic autocorrelation. We show \mathbf{s} is perfect by showing that it has the array orthogonality property (AOP) for the divisor 2. First, we show that the cross-correlation of the two columns of \mathbf{S} is zero for every non-zero shift.

$$\theta_{S_{i,0}, S_{i,1}}(\kappa) = \sum_{i=0}^{2mn^{k+1}-1} S_{i,0} S_{i+\kappa,1}^* \quad (1)$$

Let $i = qn + r$, ($r < n$), and $\kappa = q'n + r'$, ($r' < n$), then (1) becomes

$$\begin{aligned} \theta_{S_{qn+r,0}, S_{qn+r,1}}(q'n + r') &= \sum_{q=0}^{2mn^k-1} \sum_{r=0}^{n-1} S_{qn+r,0} S_{(q+q')n+r+r',1}^* \\ &= \sum_{q=0}^{2mn^k-1} \sum_{r=0}^{n-1} \omega^{\left\lfloor \frac{(qn+r)^2}{n} \right\rfloor} \omega^{\left\lfloor \frac{((q+q')n+r+r')^2 + (q+q')n+r+r'}{n} \right\rfloor} \\ &= \sum_{q=0}^{2mn^k-1} \sum_{r=0}^{n-1} \omega^{-(2nq'+2r'+1)q - 2q'r + \left\lfloor \frac{r^2}{n} \right\rfloor - \left\lfloor \frac{(r+r')(r+r'+1)}{n} \right\rfloor} \\ &= \omega^{-2q'r' - q'} \left(\sum_{q=0}^{2mn^k-1} \omega^{-(2nq'+2r'+1)q} \right) \left(\sum_{r=0}^{n-1} \omega^{-2q'r + \left\lfloor \frac{r^2}{n} \right\rfloor - \left\lfloor \frac{(r+r')(r+r'+1)}{n} \right\rfloor} \right). \end{aligned}$$

The leftmost summation above is zero, as $-2nq' - 2r' - 1 \not\equiv 0 \pmod{2mn^k}$ (since $-2nq' - 2r' - 1$ is odd for all n, q', r' , whereas $2mn^k$ is even for all n, q', r'). Thus \mathbf{s} satisfies the first condition of the AOP.

Now we show that \mathbf{s} satisfies the second condition of the AOP. That is, for all non-zero shifts, we show that the sum of the periodic autocorrelations of both columns of \mathbf{S} sums to zero.

$$\begin{aligned} \theta_{S_{i,0}}(\kappa) + \theta_{S_{i,1}}(\kappa) &= \sum_{i=0}^{2mn^{k+1}-1} S_{i,0} S_{i+\kappa,0}^* + \sum_{i=0}^{2mn^{k+1}-1} S_{i,1} S_{i+\kappa,1}^* \\ &= \sum_{i=0}^{2mn^{k+1}-1} \omega^{\left\lfloor \frac{i^2}{n} \right\rfloor} \omega^{\left\lfloor \frac{(i+\kappa)^2}{n} \right\rfloor} + \sum_{i=0}^{2mn^{k+1}-1} \omega^{\left\lfloor \frac{i^2+i}{n} \right\rfloor} \omega^{\left\lfloor \frac{(i+\kappa)^2+i+\kappa}{n} \right\rfloor} \quad (2) + (3) \end{aligned}$$

Let $i = qn + r$, ($r < n$), and $\kappa = q'n + r'$, ($r' < n$), then (2) becomes

$$\begin{aligned} &\omega^{-2q'r' - nq'^2} \sum_{q=0}^{2mn^k-1} \sum_{r=0}^{n-1} \omega^{-2(nq'+r')q - 2q'r + \left\lfloor \frac{r^2}{n} \right\rfloor - \left\lfloor \frac{r^2+r'^2+2r'r}{n} \right\rfloor} \\ &= \omega^{-2q'r' - nq'^2} \left(\sum_{q=0}^{2mn^k-1} \omega^{-2(nq'+r')q} \right) \left(\sum_{r=0}^{n-1} \omega^{-2q'r + \left\lfloor \frac{r^2}{n} \right\rfloor - \left\lfloor \frac{r^2+r'^2+2r'r}{n} \right\rfloor} \right). \quad (4) \end{aligned}$$

Similarly, (3) becomes

$$\begin{aligned} &\omega^{-2q'r' - nq'^2 - q'} \sum_{q=0}^{2mn^k-1} \sum_{r=0}^{n-1} \omega^{-2(nq'+r')q - 2q'r + \left\lfloor \frac{r^2+r}{n} \right\rfloor - \left\lfloor \frac{r^2+2r'r+r+r'^2+r'}{n} \right\rfloor} \\ &= \omega^{-2q'r' - nq'^2 - q'} \left(\sum_{q=0}^{2mn^k-1} \omega^{-2(nq'+r')q} \right) \left(\sum_{r=0}^{n-1} \omega^{-2q'r + \left\lfloor \frac{r^2+r}{n} \right\rfloor - \left\lfloor \frac{r^2+2r'r+r+r'^2+r'}{n} \right\rfloor} \right). \quad (5) \end{aligned}$$

Then $\theta_{S_{i,0}}(\kappa) + \theta_{S_{i,1}}(\kappa) = (4) + (5)$ is given by

$$\omega^{-2q'r'-nq'^2} \left(\sum_{q=0}^{2mn^k-1} \omega^{-2(nq'+r')q} \right) \left(\sum_{r=0}^{n-1} \omega^{-2q'r + \lfloor \frac{r^2}{n} \rfloor - \lfloor \frac{r^2+r'^2+2r'r}{n} \rfloor} + \omega^{-q'} \sum_{r=0}^{n-1} \omega^{-2q'r + \lfloor \frac{r^2+r}{n} \rfloor - \lfloor \frac{r^2+2r'r+r+r'^2+r'}{n} \rfloor} \right).$$

The summation $\sum_{q=0}^{2mn^k-1} \omega^{-2(nq'+r')q}$ is non-zero when $-2(nq' + r') = 0 \pmod{2mn^k}$, which is when $q' = -mn^{k-1}$, $r' = 0$ (excluding $q' = r' = 0$ as we only consider off-peak autocorrelations). In which case we have

$$\sum_{r=0}^{n-1} \omega^{-2q'r + \lfloor \frac{r^2}{n} \rfloor - \lfloor \frac{r^2+r'^2+2r'r}{n} \rfloor} = \sum_{r=0}^{n-1} \omega^{-2q'r + \lfloor \frac{r^2+r}{n} \rfloor - \lfloor \frac{r^2+2r'r+r+r'^2+r'}{n} \rfloor} =$$

$$\sum_{r=0}^{n-1} \omega^{-2q'r} = \sum_{r=0}^{n-1} e^{\left(\frac{2\pi\sqrt{-1}}{n}\right)r} = 0.$$

Thus, $\theta_{S_{i,0}}(\kappa) + \theta_{S_{i,1}}(\kappa) = 0$, so \mathbf{s} satisfies the second condition of the AOP. It follows that \mathbf{s} is a perfect sequence.

We note that the array, \mathbf{S} , also has perfect periodic autocorrelation. The proof follows from the sequence, \mathbf{s} , having the AOP.

In terms of the ratio of the sequence length to the number of phases, this construction sits below the construction of Milewski and above the constructions of Chu and Liu.

References

- [Alltop, 1980] W. O. Alltop, “Complex sequences with low periodic correlations”, *IEEE Trans. Inform. Theory*, vol. IT-26, no. 3, pp. 350-354, May 1980
- [Blake, 2012] S. T. Blake, A. Z. Tirkel, “A Construction for Periodic ZCZ Sequences”, submitted for publication, December 2012
- [Chu, 1972] D. C. Chu, “Polyphase Codes With Good Periodic Correlation Properties”, *IEEE transactions on information theory*, vol. 18, no. 4, pp. 531-532, July 1972
- [Farnett, 1990] E. C. Farnett et al, “Pulse Compression Radar” *Radar Handbook, 2nd edition, Skolnik, M., Ed., McGraw-Hill*, 1990
- [Frank, 1962] R. L. Frank, S. A. Zadoff and R. Heimiller, “Phase Shift Pulse Codes with Good Periodic Correlation Properties”, *IRE Transactions on Information Theory*, vol. 8, no. 6, pp. 381-382, October 1961
- [Gabidulin, 1993] E. M. Gabidulin, “Non-binary sequences with perfect periodic auto-correlation and with optimal periodic cross-correlation”, *Proc. IEEE Int. Symp. Inform. Theory*, San Antonio, USA, pp. 412, January 1993
- [Heimiller, 1961] R. C. Heimiller, “Phase Shift Pulse Codes with Good Periodic Correlation Properties”, *IRE Transactions on Information Theory*, vol. 7, no. 4, pp. 254-257, October 1961
- [Ipatov, 1979] V. P. Ipatov, “Ternary sequences with ideal autocorrelation properties”, *Radio Eng. Electron. Phys.*, vol. 24, pp. 75-79, October 1979
- [Ipatov, 2005] V. P. Ipatov, “Spread Spectrum and CDMA: Principles and Applications”, *John Wiley & Sons*, 2005

- [Kumar, 1985] P. V. Kumar, R. A. Scholtz, L. R. Welch, “Generalized Bent functions and their properties”, *J. Combinat. Theory, series A*, vol. 40, no. 1, pp. 90-107, 1985
- [Lewis, 1982] B. L. Lewis, F. F. Kretschmer, “Linear frequency modulation derived polyphase pulse compression”, *IEEE Trans. on AES*, vol. AES-18, no. 5, pp. 637-641, September 1982
- [Liu, 2004] Y. Liu and P. Fan, “Modified Chu sequences with smaller alphabet size”, *Electronics Letters*, vol. 40, no. 10, May 2004
- [Milewski, 1983] A. Milewski, “Periodic Sequences with Optimal Properties for Channel Estimation and Fast Start-Up Equalization”, *IBM Journal of Research and Development*, vol. 27, no. 5, pp. 426-431, September 1983
- [Mow, 1993] W. H. Mow, “A Study of Correlation of Sequences”, PhD, Department of Information Engineering, The Chinese University of Hong Kong, 1993
- [Simon, 1985] M. K. Simon, “Spread spectrum communications, Volume 1”, *Computer Science Press, The University of Michigan*, 1985
- [Tirkel, 1993] A. Z. Tirkel, G. A. Rankin, R. M. Van Schyndel, W. J. Ho, N. R. A. Mee, C. F. Osborne, “Electronic Water Mark”, *DICTA 93*, Macquarie University, pp. 666-673, 1993
- [Van Schyndel, 2001] R. G. Van Schyndel “Using Phase-Modulated Probe Signals to Recover Delays from Higher Order Non-linear Systems”, *IEEE Engineering in Medicine and Biology: Biomedical Research in 2001*, pp. 94-97, February 2001
- [Xu, 2011] L. Xu, “Phase coded waveform design for Sonar Sensor Network”, *Conference on Communications and Networking in China (CHINACOM), 2011 6th International ICST*, pp. 251-256, August 2011